

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problems Mailbox.**



## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **07038599 A**(43) Date of publication of application: **07 . 02 . 95**

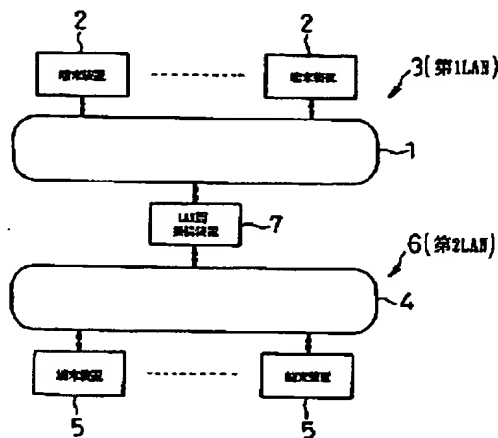
(51) Int. Cl. **H04L 12/46**  
**H04L 12/28**  
**G06F 13/00**  
**G06F 15/16**

(21) Application number: **05179404**(71) Applicant: **TOSHIBA CORP**(22) Date of filing: **20 . 07 . 93**(72) Inventor: **TATARA HIROYUKI****(54) INTER-LAN CONNECTOR****(57) Abstract:**

**PURPOSE:** To prevent data from being illegally accessed from a LAN on a low security side to a LAN on a high security side when connecting the LAN at different security levels.

**CONSTITUTION:** When the data are accessed from each terminal equipment 5 constituting a second LAN 6 at the high security level to each terminal equipment 2 constituting a first LAN 3 at the low security level, this is detected by the transport layer of an inter-LAN connector 7, the data access between these respective terminal equipments 2 and 5 is supported, when the data are oppositely accessed from each terminal equipment 2 to each terminal equipment 5, this is detected by the transport layer of the inter-LAN connector 7, and the data access between these respective terminal equipments 2 and 5 is inhibited.

COPYRIGHT: (C)1995,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-38599

(43) 公開日 平成7年(1995)2月7日

(51) Int.Cl. <sup>6</sup>	識別記号	片内整理番号	F I	技術表示箇所
H 0 4 L 12/46				
12/28				
G 0 6 F 13/00	3 5 1 Z	7368-5B		
15/16	4 7 0 M	7429-5L		
		8732-5K		
			H 0 4 L 11/ 00	3 1 0 C
			審査請求	未請求 請求項の数1 O L (全 9 頁)

(21) 出願番号 特願平5-179404

(22) 出願日 平成5年(1993)7月20日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 多々良 裕之

東京都港区芝浦一丁目1番1号 株式会社

東芝本社事務所内

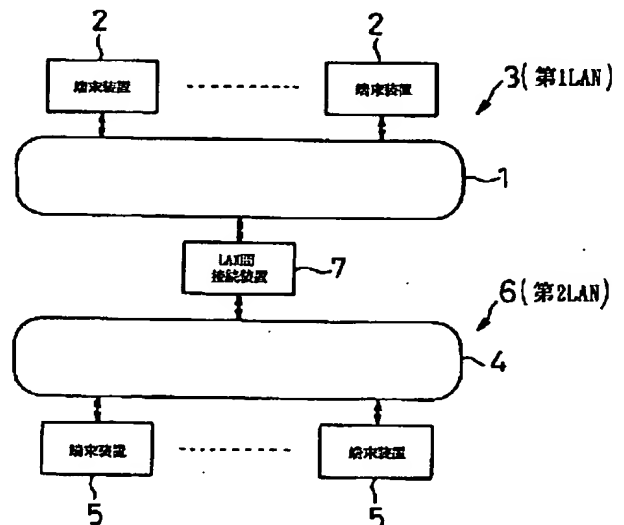
(74) 代理人 弁理士 三好 秀和 (外3名)

#### (54) 【発明の名称】 LAN間接続装置

#### (57) 【要約】

【目的】 本発明はセキュリティレベルが異なるLAN間を接続するとき、低セキュリティレベル側のLANから高セキュリティレベル側のLANに対する不正なデータアクセスを防止する。

【構成】 セキュリティレベルが高い第2LAN6を構成する各端末装置5からセキュリティレベルが低い第1LAN3を構成する各端末装置2に対するデータアクセスがあったとき、LAN間接続装置7のトランスポート層23によってこれを検出してこれらの各端末装置2、5間のデータアクセスをサポートし、逆に前記各端末装置2から前記各端末装置5に対するデータアクセスがあったとき、LAN間接続装置7のトランスポート層23によってこれを検出してこれらの各端末装置2、5間のデータアクセスを禁止する。



## 【特許請求の範囲】

【請求項1】 OSI規格によって指定された複数の層を有し、セキュリティが高く設定された高セキュリティLANと、OSI規格によって指定された複数の層を有し、セキュリティが低く設定された低セキュリティLANとを接続するLAN間接続装置において、  
処理層としてOSI規格の物理層、データリンク層、ネットワーク層、トランスポート層を備え、  
低セキュリティLANを構成する端末装置の1つから高セキュリティLANを構成する端末装置に対して接続要求が出されたとき、前記トランスポート層によってこれを取り込んで接続要求のTCPフォーマットおよびこのTCPフォーマット中の確立要求フラグの有無を確認し、接続要求を出した端末装置と、接続先として指定された端末装置との間のコネクションを禁止し、  
高セキュリティLANを構成する端末装置の1つから低セキュリティLANを構成する端末装置に対して接続要求が出されたとき、前記トランスポート層によってこれを取り込んで接続要求のTCPフォーマットおよびこのTCPフォーマット中の確立要求フラグの有無を確認し、正しい接続要求であれば、接続要求を出した端末装置と、接続先として指定された端末装置との間のコネクションを確立してデータ通信を行なわせる、  
ことを特徴とするLAN間接続装置。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】本発明は複数のLANを接続して情報処理ネットワークシステムを構築するとき使用されるLAN間接続装置に関する。

## 【0002】

【従来の技術】LAN間接続装置を使用して複数のLANを相互に接続した情報処理ネットワークシステムとして、従来、図5に示すシステムが知られている。

【0003】この図に示す情報処理ネットワークシステムは1つのケーブル101およびこのケーブル101に接続される複数の端末装置102によって構成される第1LAN103と、1つのケーブル104およびこのケーブル104に接続される複数の端末装置105によって構成される第2LAN106と、これら第1、第2LAN103、106を相互に接続するLAN間接続装置107とを備えており、第1、第2LAN103、106に接続されている各端末装置102、105間でデータの授受を行なって各種のデータ処理を行なう。

【0004】前記第1、第2LAN103、106は各々、図6に示す如くOSI規格によって物理層110、データリンク層111、ネットワーク層112、トランスポート層113、セッション層114、プレゼンテーション層115、応用層116の7層によって構成されており、このOSI規格によって異機種のコピュータ動作を自由に、かつ相互に接続し得るようにされている。

【0005】また、LAN間接続装置107は物理層120、データリンク層121、ネットワーク層122の3層によって構成されており、これらの物理層120～ネットワーク層122によって第1LAN103の各端末装置102と、第2LAN106の各端末装置105とのデータ通信を相互にサポートする。

【0006】そして、第1LAN103を構成する端末装置102の1つから第2LAN106を構成する端末装置105に対して接続要求を出したとき、図7に示す如くLAN間接続装置107によってこれを取り込んで接続要求を出した端末装置102と、接続先として指定された端末装置105との間のコネクションを確立してデータ通信を行なわせる。

【0007】同様に、第2LAN106を構成する端末装置105の1つから第1LAN103を構成する端末装置102に対して接続要求を出したとき、LAN間接続装置107によってこれを取り込んで接続要求を出した端末装置105と、接続先として指定された端末装置102との間のコネクションを確立してデータ通信を行なわせる。

【0008】これによって、第1、第2LAN103、106の各端末装置102、105によって第1、第2LAN103、106を構成する他の各端末装置102、105内のデータを参照したり、より大規模なデータ処理を可能にしたりしている。

## 【0009】

【発明が解決しようとする課題】しかしながら、上述した従来のLAN間接続装置107を使用した情報処理ネットワークシステムにおいては、次に述べるような問題があった。

【0010】すなわち、第1LAN103または第2LAN106の各セキュリティレベルを異なった値にしている場合、例えば第1LAN103のセキュリティレベルを低くし、第2LAN106のセキュリティレベルを高くしているとき、第2LAN106自体のセキュリティレベルを高くし、この第2LAN106を構成する各端末装置105間のデータ通信を制限していても、第1LAN103を構成する各端末装置102によって第2LAN106を構成する各端末装置105内のデータが取り込まれて第2LAN106のセキュリティが破られてしまうという保管管理上の問題があった。

【0011】そこで、このような問題を解決する方法として、LAN間接続装置107によって送信元アドレスと、宛先アドレスとを確認して第1LAN103と第2LAN106との間のデータ中継を制限する方法も試みられているが、このような方法では、アドレスが不正に改ざんされたとき、セキュリティが破られてしまうという問題があり、決定的な解決には至っていないのが現状である。

【0012】本発明は上記の事情に鑑み、セキュリティ

レベルが異なるLAN間を接続するとき、セキュリティレベルが低い方のLANからセキュリティレベルが高い方のLANに対する不正なデータアクセスを防止し、これによってセキュリティレベルが高く設定されているLANのデータが外部に漏れないようにすることができるLAN間接続装置を提供することを目的としている。

#### 【0013】

【課題を解決するための手段】上記の目的を達成するために本発明は、OSI規格によって指定された複数の層を有し、セキュリティが高く設定された高セキュリティLANと、OSI規格によって指定された複数の層を有し、セキュリティが低く設定された低セキュリティLANとを接続するLAN間接続装置において、処理層としてOSI規格の物理層、データリンク層、ネットワーク層、トランスポート層を備え、低セキュリティLANを構成する端末装置の1つから高セキュリティLANを構成する端末装置に対して接続要求が出されたとき、前記トランスポート層によってこれを取り込んで接続要求のTCPフォーマットおよびこのTCPフォーマット中の確立要求フラグの有無を確認し、接続要求を出した端末装置と、接続先として指定された端末装置との間のコネクションを禁止し、高セキュリティLANを構成する端末装置の1つから低セキュリティLANを構成する端末装置に対して接続要求が出されたとき、前記トランスポート層によってこれを取り込んで接続要求のTCPフォーマットおよびこのTCPフォーマット中の確立要求フラグの有無を確認し、正しい接続要求であれば、接続要求を出した端末装置と、接続先として指定された端末装置との間のコネクションを確立してデータ通信を行なわせることを特徴としている。

#### 【0014】

【作用】上記の構成において、処理層としてOSI規格の物理層、データリンク層、ネットワーク層、トランスポート層を備え、低セキュリティLANを構成する端末装置の1つから高セキュリティLANを構成する端末装置に対して接続要求が出されたとき、前記トランスポート層によってこれを取り込んで接続要求のTCPフォーマットおよびこのTCPフォーマット中の確立要求フラグの有無を確認し、正しい接続要求であれば、接続要求を出した端末装置と、接続先として指定された端末装置との間のコネクションを禁止し、高セキュリティLANを構成する端末装置の1つから低セキュリティLANを構成する端末装置に対して接続要求が出されたとき、前記トランスポート層によってこれを取り込んで接続要求のTCPフォーマットおよびこのTCPフォーマット中の確立要求フラグの有無を確認し、正しい接続要求であれば、接続要求を出した端末装置と、接続先として指定された端末装置との間のコネクションを確立してデータ通信を行なわせることにより、セキュリティレベルが異なるLAN間を接続するとき、セキュリティレベルが低い方のLANからセキュリ

ティレベルが高い方のLANに対する不正なデータアクセスを防止し、これによってセキュリティレベルが高く設定されているLANのデータが外部に漏れないようにする。

#### 【0015】

【実施例】図1は本発明によるLAN間接続装置の一実施例を使用した情報処理ネットワークシステムの一例を示すブロック図である。

【0016】この図に示す情報処理ネットワークシステムは1つのケーブル1およびこのケーブル1に接続される複数の端末装置2によって構成され、セキュリティレベルが低く設定される第1LAN3と、1つのケーブル4およびこのケーブル4に接続される複数の端末装置5によって構成され、セキュリティレベルが高く設定される第2LAN6と、これら第1、第2LAN3、6を相互に接続するLAN間接続装置7とを備えており、第1LAN3を構成する端末装置2間でデータの授受を行なって各種のデータ処理を行なうとともに、第2LAN6を構成する端末装置5間でデータの授受を行なって各種のデータ処理を行ない、さらに第2LAN6を構成する各端末装置5から第1LAN3を構成する各端末装置2に対するデータアクセスをサポートし、逆に第1LAN3を構成する各端末装置2から第2LAN6を構成する各端末装置5に対するデータアクセスを禁止する。

【0017】前記第1、第2LAN3、6は各々、図2に示す如くOSI規格によって物理層10、データリンク層11、ネットワーク層12、トランスポート層13、セッション層14、プレゼンテーション層15、応用層16の7層によって構成されており、このOSI規格によって異機種種のコンピュータ動作を自由に、かつ相互に接続し得るようにされている。

【0018】また、LAN間接続装置7は物理層20、データリンク層21、ネットワーク層(IP層)22、トランスポート層(TCP層)23の4層によって構成されており、これらの物理層20～トランスポート層23によって第2LAN6の各端末装置5から第1LAN3の各端末装置2に対するデータアクセスをサポートしている。

【0019】この場合、図3に示す如くこれら第1、第2LAN3、6およびLAN間接続装置7を構成する各物理層10、20はOSI参照モデルの第1層を構成する層であり、同軸ケーブルや光ファイバ、通信衛星の採用、アナログ伝送方式に加え、デジタル伝送の導入などにより、データの伝送路、すなわち通信媒体の多様化が進んでいることから、この多様な通信媒体の制御機能を物理層として分離して、通信媒体の選択の自由度を増すために設けられている。

【0020】また、データリンク層11、21はOSI参照モデルの第2層にあたる層であり、1本の通信媒体上で単位データを転送する際、通信媒体の誤り品質や形

10

20

30

40

50

状（直通、分岐、ループなど）などに対して特別の制御技術が必要になることから、今後、光ファイバや通信衛星の普及に対応して、従来のデータリンク制御手順（HDLCやベーシック手順など）に代わり、特有の最適なデータリンク制御手順が開発される可能性があり、通信媒体の制御（物理層）とその上のデータリンク転送制御を別々の機能層としておくことが適切であることから設けられている。

【0021】また、ネットワーク層12、22はOS I参照モデルの第3層にあたる層であり、一般に大規模で複雑な構成のコンピュータネットワークにおいては、通信の終端として動作する開放型システム（すなわち、応用プロセスが存在する開放型システム）間には、並列あるいは直列に使用されている通信回線網や、通信の中継の役割を果たす開放型システムが存在し、またある開放型システムが終端開放型システムとしても、中間開放型システムとしても動作する場合があることから、このとき必要となるデータ転送中継の機能を、直結された開放型システム間データを転送する機能（データリンク層）と独立させ、その上位に位置づけておくのが適切であることから設けられている。

【0022】また、トランスポート層13、23はOS I参照モデルの第4層にあたる層であり、ネットワーク層12、22によって構成の複雑なコンピュータネットワークにおいても、終端開放型システムでも、そのネットワークを意識することなく通信を行うことが可能であるものの、通信回線網によっては、転送誤り率やスループットなどサービス品質にばらつきがあるため、そのままでは適用業務が必要とする品質のサービスを提供できないことがあることから、これを補完し、かつ種々の通信網を利用して開放型システム間接続を可能にするためには、ネットワーク層12、22の上位に終端開放型システム間でのデータ転送制御を実現する機能層が必要になることから設けられている。

【0023】また、セッション層14はOS I参照モデルの第5層にあたる層であり、トランスポート層13以下の機能によって開放型システム間の効率の良いデータ転送が可能であるものの、応用プロセスが意味のある通信を行うためにはさらに、応用プロセス間で合意された一定のルールに従って秩序正しくデータを送受信する機構、すなわちトランスポート層13の上位に、業務の目的に合わせて応用プロセス間で種々の形態の対話を可能する機能が必要になることから設けられている。

【0024】また、プレゼンテーション層15はOS I参照モデルの第6層にあたる層であり、セッション層14を利用すれば応用プロセス間でのデータの送受信は可能になるものの、応用プロセスがそのデータを正しく処理するためには、データの表現形式（符号・キャラクタセット、データ圧縮、暗号など）に対する解釈の相違が発生しないようにする必要、すなわちセッション層14の上

位の機能層として、データの表現形式の折衝・識別・解釈などを行い、必要に応じて表現形式の変換も行う機構を設定しておく必要があることから、このデータ表現形式制御の機能として、データの意味内容を扱う機能と切り離しておくのが適当であり、これによってデータの意味内容を変更することなく、適切な表現形式を採択してデータを送受信することが可能になることから設けられている。

【0025】また、応用層16はOS I参照モデルの第7層にあたる層であり、応用プロセス間で送受信されるデータの意味内容に対応した通信処理機能を行うのみならず、通常の適用業務では、資源利用機能（例えばファイル転送・アクセス、データベースアクセス、仮想端末アクセス、メールボックスアクセスなど）と、コンピュータネットワークの運転制御に必要なネットワーク管理機能（開放型システムや物理媒体などに対する障害管理、構成管理など）とを必要とすることから、応用プロセスの処理内容に対応した通信処理機能として、データの意味内容にかかわらないプレゼンテーション層15以下の層に対し、別の機能層として設定しておく必要があることから設けられている。

【0026】そして、セキュリティレベルが低い第1 LAN3を構成する端末装置2の1つからセキュリティレベルが高い第2 LAN6を構成する端末装置5に対して接続要求を出したとき、図4に示す如くLAN間接続装置7のトランスポート層23によってこれを取り込んで接続要求のTCPフォーマットおよびこのTCPフォーマット中の確立要求フラグの有無を確認するとともに、この確認結果に関わらず接続要求を出した端末装置2と、接続先として指定された端末装置5との間のコネクションを禁止する。

【0027】逆に、セキュリティレベルが高い第2 LAN6を構成する端末装置5の1つからセキュリティレベルが低い第1 LAN3を構成する端末装置2に対して接続要求を出したとき、LAN間接続装置7のトランスポート層23によってこれを取り込んで接続要求のTCPフォーマットおよびこのTCPフォーマット中の確立要求フラグの有無を確認し、正しい接続要求であれば、接続要求を出した端末装置5と、接続先として指定された端末装置2との間のコネクションを確立してデータ通信を行なわせる。

【0028】これによって、第2 LAN6の各端末装置5によって第1 LAN3を構成する他の各端末装置2内のデータを参照したり、より大規模なデータ処理を可能にしたりする。

【0029】このようにこの実施例においては、セキュリティレベルが高い第2 LAN6を構成する各端末装置5からセキュリティレベルが低い第1 LAN3を構成する各端末装置2に対するデータアクセスがあったとき、LAN間接続装置7のトランスポート層23によってこ

れを検出してこれらの各端末装置 2、5 間のデータアクセスをサポートし、逆にセキュリティレベルが低い第 1 LAN 3 を構成する各端末装置 2 からセキュリティレベルが高い第 2 LAN 6 を構成する各端末装置 5 に対するデータアクセスがあったとき、LAN 間接続装置 7 のトランスポート層 2 3 によってこれを検出してこれらの各端末装置 2、5 間のデータアクセスを禁止するようにしたので、セキュリティレベルが異なる LAN 間を接続するとき、セキュリティレベルが低い方の LAN からセキュリティレベルが高い方の LAN に対する不正なデータアクセスを防止し、これによってセキュリティレベルが高く設定されている LAN のデータが外部に漏れないようにすることができる。

**【 0 0 3 0 】**

【発明の効果】以上説明したように本発明によれば、セキュリティレベルが異なるLAN間を接続するとき、セキュリティレベルが低い方のLANからセキュリティレベルが高い方のLANに対する不正なデータアクセスを防止し、これによってセキュリティレベルが高く設定されているLANのデータが外部に漏れないようにすることができる。

【図面の簡単な説明】

【図１】本発明によるＬＡＮ間接続装置の一実施例を使用した情報処理ネットワークシステムの一例を示すブロック図である。

【図２】図１に示す第１、第２ＬＡＮおよびＬＡＮ間接続装置の構成例を示す模式図である。

(5)

8

\* 【図3】図1に示す第1、第2LANおよびLAN間接続装置の各層を説明するための模式図である。

【図4】図1に示す情報処理ネットワークシステムの動作例を示す模式図である。

【図5】従来から知られているLAN間接続装置を使用した情報処理ネットワークシステムの一例を示すブロック図である。

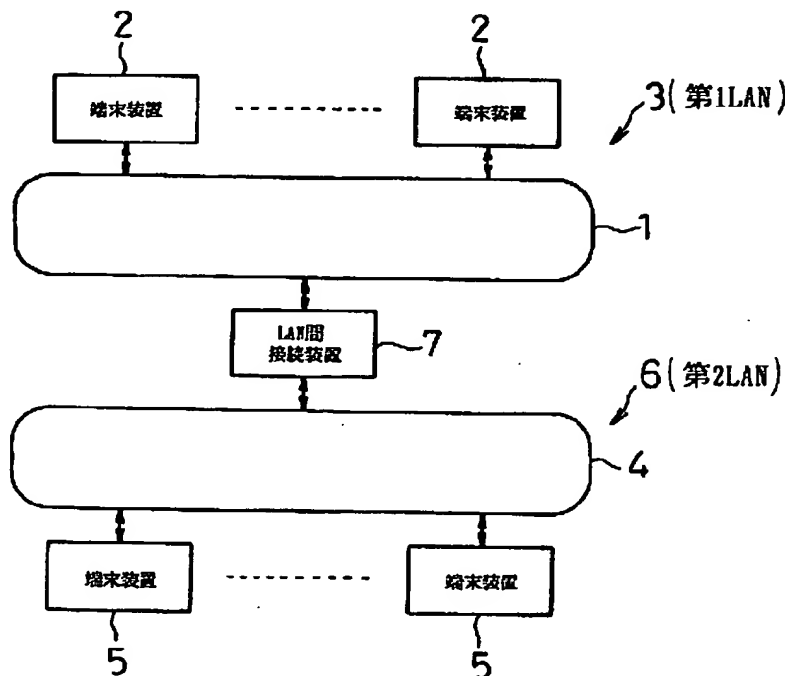
【図6】図5に示す第1、第2LANおよびLAN間接続装置の構成例を示す模式図である。

【図7】図5に示す情報処理ネットワークシステムの動作例を示す模式図である。

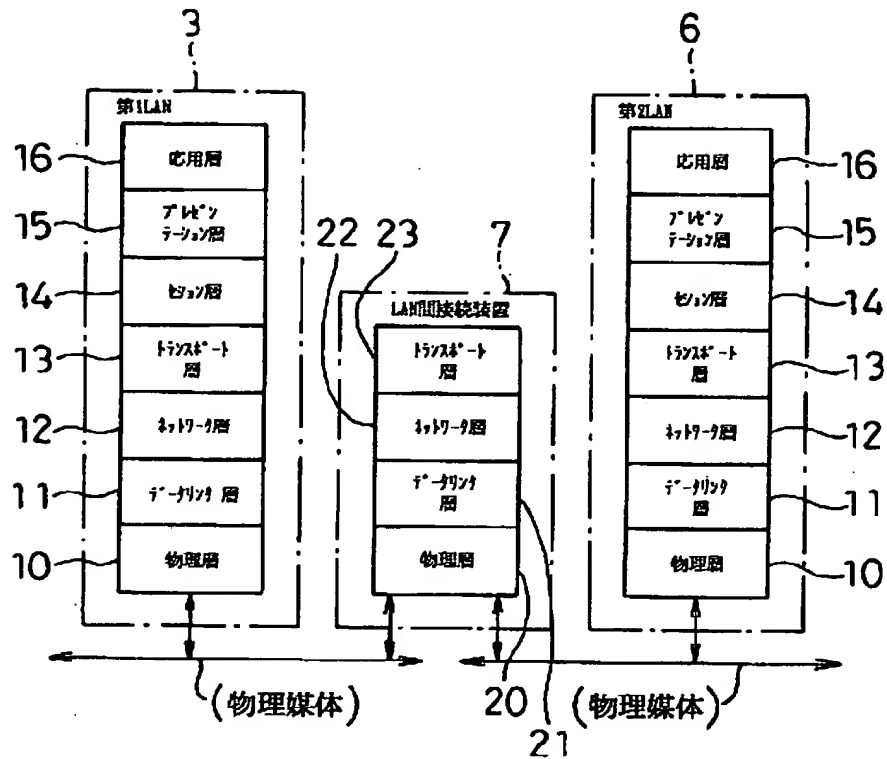
【符号の説明】

- 1 ケーブル
- 2 端末装置
- 3 第1 LAN (低セキュリティ LAN)
- 4 ケーブル
- 5 端末装置
- 6 第2 LAN (高セキュリティ LAN)
- 7 LAN間接続装置
- 10、20 物理層
- 11、21 データリンク層
- 12、22 ネットワーク層
- 13、23 トランスポート層
- 14 セッション層
- 15 プレゼンテーション層
- 16 応用層

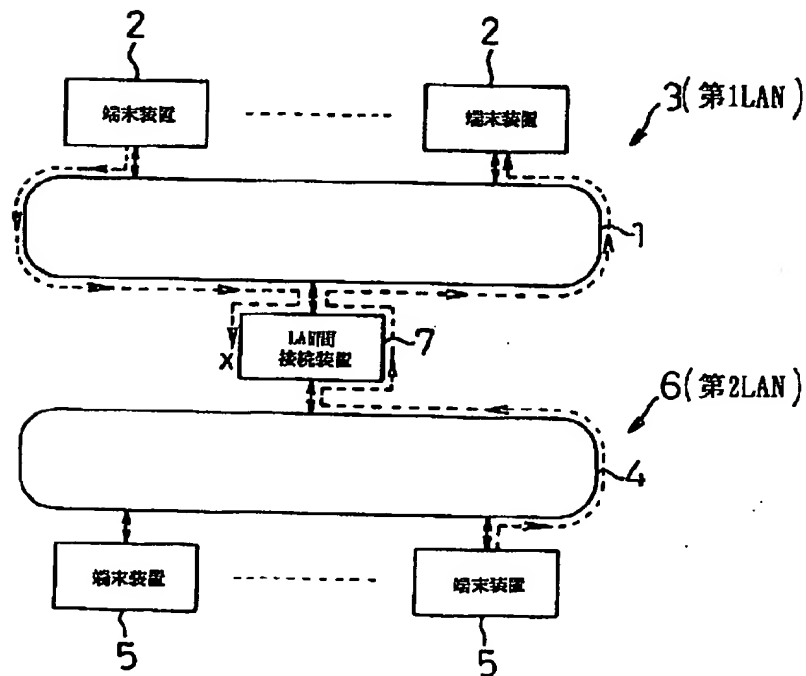
【図 1】



【図2】

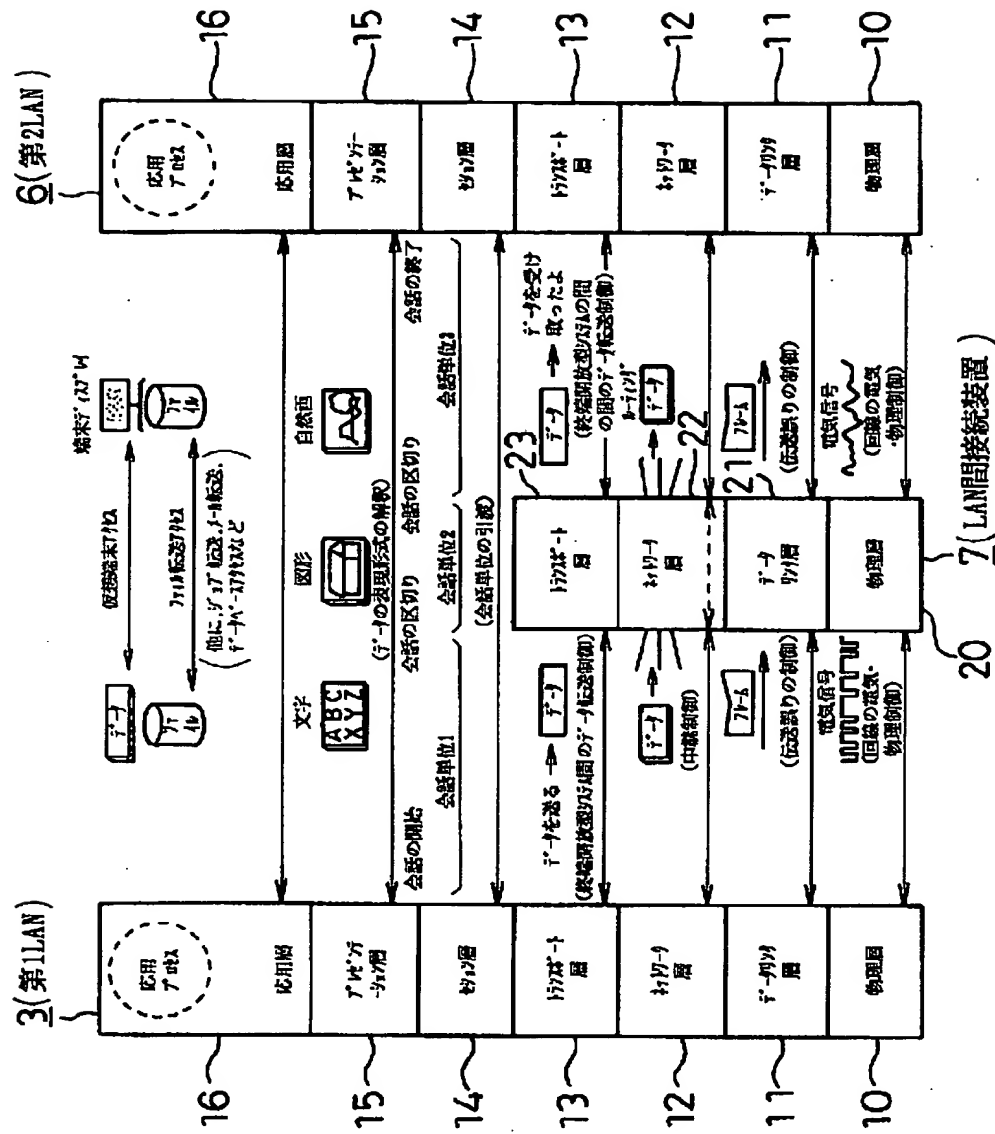


【図4】

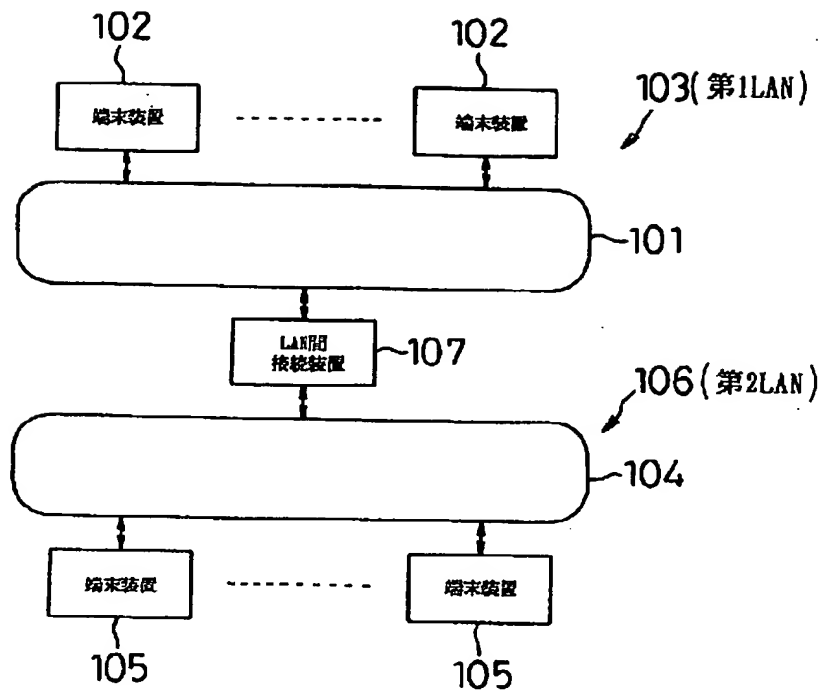




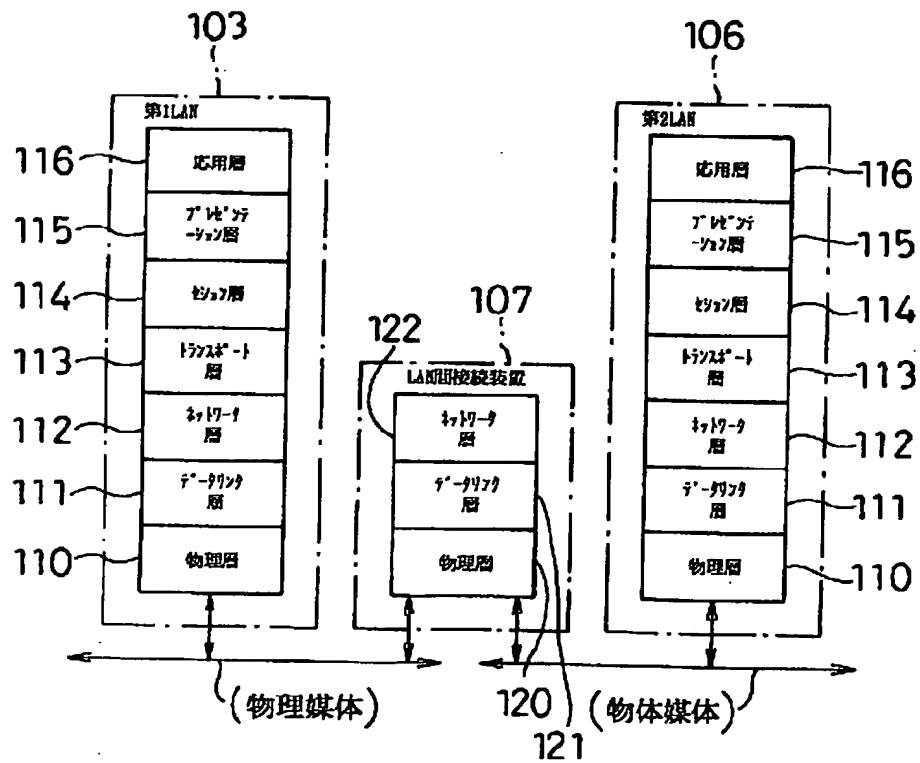
【図3】



【図5】



【図6】



【図7】

